ABSTRACT OF THE DISCLOSURE

The present invention provides a method, system, and computer program product for efficiently generating pseudo-random bits. A value which has a relatively short length is used as input to a generator function. In a preferred embodiment, the generator is a 1-way function based on the discrete logarithm with short exponent, or "DLSE", problem. Preferably, the generator function uses modular exponentiation of a fixed base, modulo a safe prime number. In particular, the function may be G^x modulo P where the length of x is at least 160 bits and the length of the output at each iteration is at least 1024 bits. Thus, any 160 of the 1024 bits can be selected for use as input to the next iteration, while producing 864 pseudo-random bits per iteration. This generator exhibits an improved rate, faster computation time, and/or reduced storage requirements as contrasted to prior art generators based on the DLSE. Precomputation tables may be used, if desired, for even better efficiency.